Department of Homeland Security Daily Open Source Infrastructure Report for 21 June 2006

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Associated Press reports Equifax Inc., one of the nation's three major credit bureaus, said Tuesday, June 20, that a company laptop containing employee names and Social Security numbers was stolen from an employee who was traveling by train near London. (See item 13)
- The Tampa Bay Business Journal reports the Tampa Port Authority has received a $1.3 million grant that will be used to purchase floating small craft intrusion barriers to protect security zones around critical infrastructure. (See item 20)
- United Press International reports Human Genome Sciences say it has sold the federal government 20,000 courses of its anthrax drug to be placed in the Strategic National Stockpile for use in the event of a bioterror attack. (See item 30)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard
Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS Daily Report Contact Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *June 19, Nuclear Regulatory Commission* — **Nuclear Regulatory Commission creates new Office of National Materials Program.** The Nuclear Regulatory Commission is reorganizing its Office of Nuclear Materials Safety and Safeguards (NMSS) and Office of State and Tribal Programs to create a new Office of National Materials Program (ONMP) and a new NMSS that

will focus on fuel cycle issues. The Office of State and Tribal Programs and the current NMSS divisions of Industrial and Medical Nuclear Safety, and Waste Management and Environmental Protection will merge and integrate their functions to form the new ONMP. The new NMSS will retain the divisions of Fuel Cycle Safety and Safeguards, High−Level Waste and Repository Safety, and the Spent Fuel Project Office, providing regulatory oversight of the entire domestic nuclear fuel cycle, from cradle to grave. NMSS will take the lead for domestic and international safeguards policy and regulation, including material control and accountability for fuel cycle facilities, which has recently been the responsibility of the Office of Nuclear Security and Incident Response. The reorganization is scheduled to be effective October 1.
Source: http://www.nrc.gov/reading−rm/doc−collections/news/2006/06−0 82.html

2. *June 19, Reuters* — **Two U.S. Gulf Coast refineries hit by storms.** At least two U.S. Gulf Coast refineries said on Monday, June 19, their production was interrupted by heavy rainstorms in Texas and Louisiana. Citgo Petroleum Corp. said on Monday it was restarting process units at its 440,000−barrel per day (bpd) refinery in Lake Charles, Louisiana, which malfunctioned due to heavy rains on Monday morning. In Port Arthur, TX, Total SA said its 234,000 bpd refinery was operating normally Monday after four units were shut and six units had production reduced due to flooding Sunday. Also in Port Arthur, Valero Energy Corp. was working to restart a blower on a gasoline−producing fluidic catalytic cracking unit (FCC) at its 210,000 bpd refinery. The FCC blower failure had no material impact to production. Weather was not the only issue causing Gulf Coast refinery troubles. Exxon Mobil Corp. was working to restart a shut gasoline−producing FCC at its 563,000 bpd refinery in Baytown, Texas, on Monday. The FCC shutdown on Friday after an overhaul that began in early May. At Shell Oil Co.'s complex in Deer Park, TX, the company cancelled a shelter−in−place order for nearby residents, triggered when benzene−rich pyrolysis gas was released from a storage tank on Monday morning.
Source: http://today.reuters.com/stocks/QuoteCompanyNewsArticle.aspx?view=CN&storyID=2006−06−19T212009Z_01_N19406878_RTRIDST_0_ENERGY−STORMS−REFINERIES.XML&rpc=66

3. *June 19, Register (UK)* — **New tidal generator could mean cheaper electricity.** Researchers at the University of Southampton in the UK have developed a new kind of marine generator they say could substantially reduce the cost of electricity generated from tidal power. Normal tidal turbines are complex pieces of kit, with lots of gears, and other moving parts that need maintaining and replacing over time. Because this new design will generate electricity whichever direction water flows through it, it has fewer parts than many turbines currently in use. This makes it cheaper to build and reduces expensive underwater maintenance. It also means less downtime, since the generators don't need to be moved to face the direction of the tidal flow. The prototype is designed so that all the components are in a single package, making it much cheaper and easier to install, the researchers say. The design may be commercially available within five years.
Source: http://www.theregister.co.uk/2006/06/19/tidal_generator/

4. *June 19, Occupational Hazards* — **Mine safety bill signed into law.** President Bush has signed into law a bill that Department of Labor Secretary Elaine Chao called "the most significant mine safety legislation in nearly 30 years." The Mine Improvement and New Emergency

Response (MINER) Act (S. 2803), requires miners to carry two hours' worth of emergency oxygen with them while they work −− up from the previous minimum of one hour −− and mandates that mine operators store extra oxygen along escape routes underground. The MINER Act also requires a mine rescue team to be located within one hour of every mine −− the previous requirement was two hours −− and calls for coal companies to put new communications and miner tracking systems in place within three years.
Source: http://www.occupationalhazards.com/articles/15316

[Return to top]

Chemical Industry and Hazardous Materials Sector

5. *June 20, Sun−Sentinel (FL)* — **Leaking propane gas tank prompts evacuations, road closure.** A leaking propane tank in Key Largo, FL, forced deputies and firefighters to shut down U.S. 1 into the Keys to all traffic and evacuate a school for several hours on Tuesday, June 20, according to the Monroe County Sheriff's Office. The area in a half−mile radius around the leaking tank was evacuated. Around noon, the road was reopened and people were allowed back into their homes and businesses.
Source: http://www.sun−sentinel.com/news/local/southflorida/sfl−620gasleak,0,4953546.story?coll=sfla−news−sfla

6. *June 20, CBS 2 (CA)* — **Tanker fire closes California interstate.** A big rig tanker rolled over, spilled 7,500 gallons of fuel and caught fire on eastbound Interstate 10 near state Route 62 in Palm Springs, CA, Tuesday morning, June 20. A U−Haul truck with three people inside also caught on fire when the driver tried to drive around the scene. All eastbound traffic was diverted to state Route 111, also known as Palm Canyon Drive.
Source: http://cbs2.com/topstories/local_story_171114321.html

7. *June 20, Associated Press* — **Train with chemicals derails in Tennessee.** A Norfolk Southern Corp. freight train with tanker cars of hazardous chemicals derailed early Tuesday, June 20, in Sweetwater, TN, leading emergency officials to evacuate dozens of residents from homes within a half mile of the accident. The train was traveling between Chattanooga and Knoxville when 21 cars went off the tracks. Norfolk Southern rerouted train traffic from the line, and U.S. 11, which runs near the tracks, was closed until Wednesday, June 21.
Source: http://hosted.ap.org/dynamic/stories/T/TRAIN_DERAILMENT?SITE=WUSA&SECTION=HOME&TEMPLATE=DEFAULT

[Return to top]

Defense Industrial Base Sector

8. *June 20, Aviation Week* — **FCS performing on time, slightly under budget, officials say.** Officials with the U.S. Army's Future Combat Systems (FCS) program said Monday, June 19, that since the program's 2004 restructuring it has been performing on schedule, and currently is running about 1 percent under budget. Nonetheless, defense appropriators in the House have voted to cut $326 million from the program's fiscal 2007 budget, leaving it with about $3

billion, citing development and contracting delays. The potential benefits of FCS are "impressive," lawmakers said, but the program's acquisition strategy of maturing technologies, designing systems and preparing for production concurrently is "a very high risk approach." They also cited the Government Accountability Office's continued reservations about the program. A report on the program from the Pentagon's Cost Analysis Improvement Group is expected soon.
Source: http://www.aviationnow.com/avnow/news/channel_defense_story.jsp?id=news/FCS06206.xml

9. *June 20, Government Accountability Office* — **GAO−06−725R: Improvement Continues in DoD's Reporting on Sustainable Ranges but Additional Time Is Needed to Fully Implement Key Initiatives (Correspondence).** Title III, section 366 of the Bob Stump National Defense Authorization Act for Fiscal Year 2003, required the Government Accountability Office (GAO) to provide Congress with an evaluation of the Office of the Secretary of Defense's (OSD) annual reports. In GAO's prior reports, they found that OSD's training range reports and inventories provided to Congress did not fully address several reporting requirements. For example, both previous OSD reports did not meet requirements because they did not include an assessment of current and future training range requirements; an evaluation of the adequacy of current resources, including virtual and constructive assets, to meet current and future training range requirements; or recommendations for legislative or regulatory changes to address training constraints −− although specifically required to do so by section 366. This letter, GAO's third report, summarizes their observations on the extent to which OSD's 2006 sustainable ranges report and range inventory address the requirements specified by section 366, and the department’s key initiatives to sustain its training ranges.
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−725R

10. *June 19, U.S. Air Force* — **Balancing capability portfolios key to Air Force success.** In order for the Air Force to remain a strong, viable force in the war on terror, it must work to recapitalize its fleet of aging aircraft, Air Force Vice Chief of Staff Gen. John D. W. Corley told lawmakers and defense industry insiders on Capitol Hill Wednesday, June 14. The Air Force maintains three "portfolios" of aircraft, and each performs a separate task, the general said. Those portfolios include strike aircraft; mobility aircraft; and command, control, computers, communication, intelligence, surveillance and reconnaissance aircraft. Aircraft in the strike portfolio are aging, and it is increasingly more expensive to maintain the capability those aircraft provide. The Air Force wants to retire 18 B−52s in the 2007 president's budget, and an additional 20 in the 2008 budget. The Air Force also plans to replace fighter aircraft such as the F−16 and the F−15 with the F−35 and the F−22 respectively. General Corley would like to see more C−17 aircraft in the Air Force fleet, but says that the mobility portfolio must be balanced. That means dealing with aging aircraft such as the KC−135 and the C−130. The Air Force is currently looking for a replacement for the KC−135 tanker aircraft.
Source: http://www.af.mil/news/story.asp?id=123022098

[Return to top]

Banking and Finance Sector

11.

June 20, Washington Post — **U.S. Mint giving gold investors a new option.** The U.S. Mint on Tuesday, June 20, unveiled the nation's first 24−karat gold coin. Modeled on the traditional buffalo nickel, the American Buffalo coin has a buffalo on one side and a Native American on the other. It comes in two versions, both stamped with a $50 face value but worth substantially more because they are made of pure gold. The new American Buffalo gold coin has a face value of $50 but will be worth far more. A "proof" version with a high−relief, mirror finish aimed at collectors will sell for $800, while the less flashy bullion version of the coin −− targeted at investors known as "gold bugs" −− will retail for the price of an ounce of gold plus a five to 7.5 percent markup to cover the cost of making and selling it. The U.S. Mint has sold 22−karat gold coins known as American Eagles since 1985, but Deputy Director David A. Lebryk said the new offering is aimed at investors who want coins that are pure gold. The mint will produce only 300,000 proof−quality American Buffalo coins but will mint enough bullion coins to meet demand.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/06/19/AR2006061901187.html

12. *June 20, Computing (UK)* — **UK Internet users naive to phishing scams.** UK Internet users are ill prepared to spot and avoid malicious email scams, according to a national security survey released Tuesday, June 20. The research −− released by government and business sponsored security awareness portal Get Safe Online −− says that more than 11 million UK consumers have received malicious emails aimed at tricking them into giving out bank details. But despite this some 29 percent, or eight million, UK adults are unsure what protective measures to take to combat phishing emails and in many case are totally unaware they are being directed to a fake site set up by criminals. The survey found that almost half of UK consumers would not automatically delete suspicious e−mails. More than a quarter said they 'just trusted their instincts' when it came to trying to avoid online scams.
Source: http://www.vnunet.com/computing/news/2158612/uk−internet−use rs−naive

13. *June 20, Associated Press* — **Equifax: Laptop with employee data stolen.** Equifax Inc., one of the nation's three major credit bureaus, said Tuesday, June 20, a company laptop containing employee names and Social Security numbers was stolen from an employee who was traveling by train near London. The theft, which could affect as many as 2,500 of the Atlanta−based company's 4,600 employees, happened May 29 and all employees were notified June 7, spokesperson David Rubinger said. Employee names and partial and full Social Security numbers were on the computer's hard drive, though Rubinger said it would be almost impossible for the thief to decipher the information because it was streamed together. The employee whose laptop was stolen has been disciplined for violating company policy, which prohibits storage of company information on a hard drive, Rubinger said.
Source: http://www.nytimes.com/aponline/business/AP−Equifax−Data−Loss.html?_r=1&oref=slogin

14. *June 19, InternetWeek* — **Social engineering gets smarter.** Here's a new phish: An attacker recently created a fake phishing message and, posing as a bank customer, forwarded it to the bank's security officer. When the security manager clicked the link to find the alleged phishing site, the message launched malware that highjacked his workstation. Security experts are seeing more targeted approaches, where a would−be attacker sets his sights on a key person within an organization, or on regional organizations, whose networks are typically not as secure as those

of their larger counterparts. It's all about manipulating the trust of a user: the security manager who believes the attacker is a real customer, or the receptionist who lets a "consultant" into the conference room, where then he jumps onto an open network port. The targeted attack on the security manager is more typical of today's exploits than the traditional mass−user attack, where an attacker sends out an e−mail blast to try to collect personal information. Social engineers target helpdesks. Doug Shields of Secure Network Technologies, says his team has found that helpdesks don't always check who's calling them, and can be duped into giving out a "forgotten" password or other information.
Source: http://internetweek.cmp.com/189500411

15. *June 19, Computeractive (UK)* — **UK Office of Fair Trading warns of new lottery scam using forged checks.** The UK Office of Fair Trading (OFT) is warning of a new type of lottery scam which uses counterfeit checks. The scam begins with a letter arriving in the mail from a company calling itself the Australian Lottery Corporation, using an address in Victoria, British Columbia, Canada. The letter states that the recipient has won $750,000. However, the victim is asked to first pay for taxes and insurance. To lull the victim into a false sense of security, a $4,880 check personally made out to the recipient, and allegedly drawn on a reputable American bank, is also attached to the mailing. The scammers claim this amount comes from the supposed winnings to cover these 'necessary payments' the consumer needs to make. Recipients are also asked to call an agent on a telephone number in North America for more information. The check is counterfeit but can take up to six weeks to work through the banking system. The consumer is at risk of being held liable for any funds they spend while waiting for the check to clear.
Source: http://www.computeractive.co.uk/computeractive/news/2158552/oft−warns−lottery−scam−forged

[Return to top]

Transportation and Border Security Sector

16. *June 20, Associated Press* — **Plane makes safe emergency landing in Chicago.** American Airlines Flight 1740, traveling from Los Angeles to Chicago, made an emergency landing Tuesday, June 20, at O'Hare International Airport after reporting difficulties with its front landing gear, according to the Federal Aviation Administration. The jet landed on its rear wheels and coasted before its nose touched down, sending up sparks. The plane carried 136 passengers and crew.
Source: http://www.cnn.com/2006/US/06/20/emergency.landing.ap/index. html

17. *June 20, Associated Press* — **Grenade−shaped belt buckle causes Salt Lake City airport evacuation.** A belt buckle resembling a hand grenade caused the evacuation of part of a terminal at Salt Lake City International Airport on Monday, June 19, officials said. The lobby and ticket counter areas of Terminal One were evacuated for about an hour after screeners saw a suspicious image while X−raying luggage, said Barbara Gann, a spokesperson at the airport. "It was a cast of a hand grenade, so half of a hand grenade and it appeared to be a grenade with a pin," Gann said. "It was wrapped around a bottle of cologne. So, it appeared to be an incendiary device with fuel." The package was placed in a containment unit, taken to a remote section of the airport where it was detonated and its contents revealed, she said. Gann said it

was unclear how many people might have missed flights or if flights were delayed due to the evacuation. Airport officials have identified the owner of the items, but that person was traveling ahead of his luggage and likely had no idea the trouble it caused, she said.
Source: http://www.usatoday.com/travel/news/2006−06−20−belt−buckle−e vacuation_x.htm

18. *June 20, Associated Press* — **San Francisco airport to be first to screen all passenger plane cargo.** Federal officials plan to make San Francisco International Airport (SFO) the first in the nation to screen all passenger aircraft cargo for explosives. The Department of Homeland Security, the Transportation Security Administration, and SFO officials signed an agreement Monday, June 19, to launch a $30−million pilot program later this summer, then expand it to two other unannounced airports. Lawrence Livermore Laboratory and several other national labs will help determine how best to apply existing luggage−screening procedures, such as bomb−sniffing dogs and X−ray machines, to cargo. The goal is to screen all cargo and do it without significantly delaying flights.
Source: http://www.usatoday.com/travel/flights/2006−06−20−sfo−bag−sc reening_x.htm

19. *June 20, Associated Press* — **TSA delays Registered Traveler program.** A program to let frequent flyers breeze through airports has been delayed as the government and private businesses grapple with ways to ensure retention of tough security standards. The Registered Traveler program, which has been tested at Orlando International Airport and four other airports, was supposed to be rolled out gradually starting Tuesday, June 20. But Transportation Security Administration (TSA) spokesperson Yolanda Clark said the agency was still working with private firms running the program to make certain that it "does not decrease security in any way." Registered Traveler would have allowed certain airline passengers to quickly go through a separate airport security lane if they paid a fee, passed a government background check and submitted fingerprints. The TSA wants private contractors to run the program, but said that travelers must be able to use the pass at every airport that offers it.
Source: http://www.boston.com/news/nation/washington/articles/2006/0 6/20/tsa_delays_registered_traveler_program/

20. *June 20, Tampa Bay Business Journal (FL)* — **Port to purchase intrusion barriers.** The Tampa Port Authority has received a $1.3 million grant from the Department of Homeland Security that will be used to purchase floating small craft intrusion barriers to protect security zones around critical infrastructure. Skip Volkle, legal counsel at shipper Maritrans, raised concerns about the barriers at Tuesday, June 20's board meeting, saying that no discussion had taken place with the Harbor Safety Committee. But Port of Tampa Director Richard Wainio assured maritime constituents present that "all security people involved recognize that this helps enhance security." "We may never have to use them," Wainio said of the barriers. "But we can have them in our arsenal to use them if we need to prevent an attack with improvised explosive devices, which is what they're designed to prevent." Wainio said the Port of Tampa would meet with the Harbor Safety Committee but that the impact of the devices to the maritime community was going to be minimal.
Source: http://tampabay.bizjournals.com/tampabay/stories/2006/06/19/ daily11.html

21. *June 20, Aviation Now* — **Boston Logan tests chipless baggage−tracking system.** Boston Logan airport will be the site of a pilot project to test the Secure Environment for Airport Terminal Systems (SEATS) baggage−tracking product, which combines radio frequency

identification (RFID) technology with hardware to improve airport baggage identification and tracking security at lower costs to airlines. SEATS uses Chipless Remote Identification System technology. Boston Logan will choose an airline to test the system in July, and the pilot will run for three to six months, said Mark Smithers, Vice President and chief operating officer of Boston Engineering. "…. as a chipless system, it's hacker−proof and tamper−resistant −− a security advantage for airports and other applications," Smithers added.
Source: http://www.aviationnow.com/avnow/news/channel_airports_story.jsp?id=news/BOS06206.xml

22. *June 19, USA TODAY* — **Delta plans long−haul luxury flights.** Delta Air Lines in August will launch a high−end transcontinental service, heating up competition for perk−loving long−haul fliers. The No. 3 airline, which is in bankruptcy reorganization, plans to renovate 100 of its 477 full−size jets for long−haul routes, with two cabins and digital TV and music throughout the plane. The planes, all Boeing 757s or 737s, will be equipped with 24 channels of live TV, interactive video games and MP3 audio programming offering more than 1,600 songs. The first of the upgraded planes will appear on transcontinental flights. The new transcontinental service is part of Delta's efforts in bankruptcy to not only cut costs but also boost revenue. Rival United Airlines has shown that luxury can command a high price on transcontinental routes. On Friday, June 16, United was selling a short−notice, coast−to−coast round−trip first−class ticket on its "Premium Service" for $4,631.
Source: http://www.usatoday.com/travel/flights/2006−06−19−delta−usat_x.htm

23. *June 18, Chicago Tribune* — **Metra apologizes for rush−hour delays.** Chicago's Metra officials apologized to their Burlington Northern Santa Fe (BNSF) passengers Friday, June 16, one day after the discovery of sacks of stearic acid on the tracks caused a nearly four−hour shutdown of the system's busiest line and stranded thousands of people on trains for up to three hours. The problems continued when Metra canceled some trains and rerouted others to comply with federal law that requires crews to rest for 10 hours after a 12−hour shift. Metra board Chairman Jeffrey Ladd said the delays were unacceptable. On Thursday, June 15, Metra halted service on the Chicago to Aurora, IL, BNSF Line for nearly four hours after the sacks fell off a Cicero−bound freight train, scattering them along a 27−mile stretch.
Source: http://www.chicagotribune.com/news/local/chicago/chi−0606180210jun18,1,6588033.story?coll=chi−newslocalchicago−hed

[Return to top]

Postal and Shipping Sector

24. *June 20, New Orleans City Business* — **Postal progress, but some deliveries still elusive in New Orleans.** The U.S. Postal Service (USPS) says it has put new hurricane evacuation plans in place after Katrina exposed mistakes in its old plan. Now, the USPS is confident mistakes made during Hurricane Katrina will never be repeated. After Katrina's floodwaters subsided and USPS inspectors surveyed the damage, they quickly found inherent mistakes in the evacuation policy. Nearly 200 trucks were lost, immeasurable pounds of first−class mail, including letters, checks, and bills were destroyed, and employees were hard to find. This season, USPS District Manager James Taylor believes the plan in place has covered all those bases. During a mandatory evacuation in New Orleans, mail would be received at one of two

locations outside the metropolitan area depending on the storm's path. The primary alternate site is the processing and distribution center in Baton Rouge. If heavy storm impact is expected in Baton Rouge, the mail would be transported to the secondary alternate processing and distribution center in Shreveport, LA. The evacuation of trucks and mail will begin approximately 90 hours before a hurricane is expected to make landfall. The USPS emergency plan also includes a customer phone line available for information.
Source: http://www.neworleanscitybusiness.com/viewStory.cfm?recID=15 841

[Return to top]

Agriculture Sector

25. *June 20, Reuters* — **Bird flu found in Canada.** A gosling from a Canadian backyard flock has tested positive for H5 avian flu. The bird was part of a noncommercial flock of 35 to 40 chickens, geese and ducks in the eastern province of Prince Edward Island. Not all H5 viruses are highly pathogenic and not all will cause severe disease in poultry. Canada has had low pathogenic bird flu outbreaks in the past, most recently in British Columbia in November 2005, when the low pathogenic H5N2 strain was discovered. There was a highly pathogenic case of H5N9 bird flu in 1966 and a case of high pathogenic H7N3 in 2004. Prince Edward Island, scene of the latest case, has only seven commercial chicken farms and industry officials said there are none within a six−mile radius of the affected farm. The flock where the dead gosling was found was culled and a neighboring backyard flock was quarantined.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/06/20/AR2006062000703.html

26. *June 19, U.S. Department of Agriculture* — **U.S. Department of Agriculture trains foreign scientists on avian influenza testing.** The U.S. Department of Agriculture's (USDA) Animal and Plant Health Inspection Service Administrator Ron DeHaven announced Monday, June 19, the training of 24 scientists from 19 countries on diagnostic testing for highly pathogenic Avian Influenza (HPAI). The workshop is scheduled for June 19−23 at USDA's National Veterinary Services Laboratories (NVSL) in Ames, IA. It is the third in a series of train−the−trainers workshops on HPAI testing and diagnostics. The 24 participants come from countries that have requested USDA technical assistance in HPAI testing and diagnostics. Countries participating include Argentina, Brazil, Burkina Faso, Burma, Cote d'Ivoire, Democratic Republic of Congo, Dominican Republic, Indonesia, Lebanon, Libya, Mexico, Mozambique, Oman, Pakistan, Romania, Sudan, Taiwan, Uganda, and Uruguay. Training will include hands−on lab exercises and lectures from USDA experts. The workshops are a joint effort of Iowa State University and USDA's Agricultural Research Service, Animal and Plant Health Inspection Service and the Foreign Agricultural Service.
Source: http://www.usda.gov/wps/portal/!ut/p/_s.7_0_A/7_0_1OB?contentidonly=true&contentid=2006/06/0209.xml

[Return to top]

Food Sector

27. *June 16, U.S. Food and drug Administration* — **Animal feed products recalled.** H.J. Baker & Bro. announced Friday, June 16, that in cooperation with the U.S. Food and Drug Administration (FDA) it has begun efforts to retrieve PRO−PAK WITH PORCINE MEAT AND BONE, PRO−LAK, AND PRO−AMINO II produced at its Albertville, AL, facility. These products are used as an ingredient in the manufacturing of livestock feed, including feed for dairy animals. This action is being taken to address potential risk of unintentional contamination with ruminant derived protein that may have occurred at this facility from August 2005 to June 2006. Certain mammalian protein is prohibited for use in ruminant feed. These products were distributed in bulk or bags to feed manufacturers and dairy farms in Georgia, Kentucky, Michigan, Florida, Alabama, Tennessee, Mississippi, California, and Louisiana.
Source: http://www.fda.gov/oc/po/firmrecalls/hjbaker06_06.html

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

28. *June 20, Reuters* — **Indonesian teenager dies of bird flu.** The World Health Organization (WHO) has confirmed an Indonesian teenager who died last week was infected with bird flu, a health ministry official said on Tuesday, June 20, taking the country's confirmed bird flu deaths to 39. The head of Indonesia's bird flu information center, Runizar Ruesin, said the 14−year−old boy was from south of Jakarta. Samples of the boy's lung fluid were sent to a WHO laboratory in Hong Kong for confirmation after he tested positive for bird flu locally. Local tests are not considered definitive. Indonesia has seen a steady rise in human bird flu infections and deaths since its first known outbreak of H5N1 in poultry in late 2003. The country of 220 million has an estimated 1.2 billion chickens, some 30 percent of them in the yards of homes in both rural and urban areas. The bird flu virus is endemic in poultry in nearly all of the 33 provinces in Indonesia, a country of 17,000 islands sprawling across some 3,100 miles.
Source: http://today.reuters.com/news/newsArticle.aspx?type=worldNews&storyID=2006−06−20T095735Z_01_JAK285513_RTRUKOC_0_US−BIRDFLU−INDONESIA−DEATH.xml&archived=False

29. *June 20, Reuters* — **Namibia to begin vaccination as polio spreads.** Namibia will begin a mass vaccination campaign on Wednesday, June 21, amid a worsening polio outbreak that has killed 12 people and infected at least 84 since May, officials said. Kalumbi Shangula of the Ministry of Health and Social Services said vaccine was already being distributed. "Everyone who has received vaccination shall be marked with an indelible marker as during the country's national elections," Shangula told a news conference. The polio virus has been reported in all but two of Namibia's 13 regions since the first case was detected on May 10.
Global Polio Eradication Initiative: http://www.polioeradication.org/

Source: http://www.alertnet.org/thenews/newsdesk/L19805873.htm

30. *June 20, United Press International* — **Government buys anthrax vaccine.** Human Genome Sciences said Tuesday, June 20, it sold the federal government 20,000 courses of its anthrax drug for $165 million. The drug courses will be placed in the Strategic National Stockpile for use in the event of a bioterror attack. The compound is a human monoclonal antibody to the anthrax bacteria Bacillus anthracis. The drug has been shown to have preventive and therapeutic efficacy against inhalational anthrax in animal models.
Source: http://www.upi.com/HealthBusiness/view.php?StoryID=20060620−091027−4062r

31. *June 19, Federal Computer Week* — **House appropriation mandates public access policy.** A measure passed in a House Appropriations bill for the U.S. Department of Health and Human Services would ensure that research funded by public tax dollars is readily available to the public. The bill requires scientists funded by the National Institutes of Health (NIH) to submit copies of their peer−reviewed journal manuscripts to NIH's online archive, known as PubMed Central. Those manuscripts would then have to be made available to the public for free on the PubMed Central Website within a year of publication. The provision cements an NIH policy that has been in effect for a year. The NIH public access policy currently asks NIH−funded scientists to submit their manuscripts voluntarily.
Source: http://www.fcw.com/article94956−06−19−06−Web

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

32. *June 20, Associated Press* — **Disaster experts come to learn in Florida.** Emergency responders from 12 states came to Florida on Monday, June 19, to learn how experts there handle disasters. From states as near as Georgia and as far away as Washington, participants echoed the same sentiment: Florida does disaster response right, and they want to know the secret. "Teamwork," said Dave Bujak, who organized the two−day seminar for the Florida Division of Emergency Management. Bujak's agency's concept, called State Emergency Response Team, dates back to Hurricane Andrew in 1992 when workers realized they had to fix their fragmented response system. They built what is best described as a tree: The Emergency Management Division is the trunk, and disconnected state agencies that once duplicated efforts and competed for resources during disasters are the branches.
Source: http://www.sptimes.com/2006/06/20/State/Disaster_experts_com e.shtml

33. *June 20, Los Angeles Times* — **With crime on the rise, Louisiana governor agrees to deploy National Guard to New Orleans.** Nearly 10 months after Hurricane Katrina, National Guard troops are returning to New Orleans to keep the peace in a city growing increasingly uneasy over its rising tide of crime. After six deaths over the weekend, Mayor C. Ray Nagin asked

Louisiana Governor Kathleen Babineaux Blanco at a news conference Monday, June 19, to send a contingent of National Guard troops and state troopers. Blanco agreed to send the reinforcements; the first 100 of 300 promised troops arrived in the city Tuesday, June 20. Sixty state troopers also will be deployed. The Police Department is down from a pre−Katrina strength of 1,700 officers to an effective force of about 1,370, said Lt. Michael Glasser, the police union president. They are working within a severely compromised justice system saddled with thousands of backlogged criminal trials, a dearth of jurors, and flood−damaged jails. In addition, officers must deal with issues like house break−ins and squatting in vast and largely depopulated swaths of the city. City officials said the Guard troops and state police will patrol the depopulated areas until September, freeing up local police to fight crime in more populous areas.
Source: http://www.latimes.com/news/nationworld/nation/la−na−neworleans20jun20,1,4247573.story?coll=la−headlines−nation

34. *June 14, The Infrastructure Security Partnership* — **TISP releases regional disaster resilience guide.** The Infrastructure Security Partnership (TISP) has developed a much needed resource, Regional Disaster Resilience: A Guide for Developing an Action Plan. The Guide was developed by the TISP Regional Disaster Resilience Committee, comprised of more than 100 practitioners, policy makers, and technical and scientific experts from across the nation. The Guide provides a strategy to develop the necessary level of preparedness for communities to manage major disasters in today's complex and interdependent world.
The Guide is available at: http://www.tisp.org/rdr_guide
TISP Website: http://www.tisp.org/tisp.cfm
Source: http://www.tisp.org/news/newsdetails.cfm?&newsID=944

[Return to top]

Information Technology and Telecommunications Sector

35. *June 20, Government Accountability Office* — **GAO−06−897T: Information Security: Leadership Needed to Address Weaknesses and Privacy Issues at Veterans Affairs (Testimony).** The recent information security breach at the Department of Veterans Affairs (VA), in which personal data on millions of veterans were compromised, has highlighted the importance of the department's security weaknesses, as well as the ability of federal agencies to protect personal information. Robust federal security programs are critically important to properly protect this information and the privacy of individuals. The Government Accountability Office (GAO) was asked to testify on VA's information security program, ways that agencies can prevent improper disclosures of personal information, and issues concerning notifications of privacy breaches. In preparing this testimony, GAO drew on its previous reports and testimonies, as well as on expert opinion provided in congressional testimony and other sources. To ensure that security and privacy issues are adequately addressed, GAO has made recommendations previously to VA and other agencies on implementing federal privacy and security laws. In addition, GAO has previously testified that in considering security breach notification legislation, the Congress should consider setting specific reporting requirements for agencies.
Highlights: http://www.gao.gov/highlights/d06897thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−897T

36. *June 20, Tech Web* — **Security vendors spot second Excel bug.** Just days after Microsoft confirmed that its Excel spreadsheet had an unpatched vulnerability currently being exploited by attackers, security vendors on Tuesday, June 20, reported a second zero−day bug. This proof−of−concept exploit code involves a DLL that handles hyperlinks in Excel worksheets. "The vulnerability occurs when a user follows a long URL link contained in an Excel spreadsheet," wrote Symantec in a Tuesday alert to customers of its DeepSight Threat Management System. "Since the proof of concept does not include a payload, it will cause Excel to crash."
Source: http://www.techweb.com/wire/security/189500947;jsessionid=X22Z4BPQ04OLAQSNDLPCKH0CJUNN2JVN

37. *June 19, IDG News Service* — **Hackers hit Microsoft France site.** Part of Microsoft Corp.'s French Website was taken offline by hackers, who apparently took advantage of a misconfigured server at the software vendor's Web hosting provider. The experts.microsoft.fr Website was defaced Sunday, June 18, with the word "HACKED!" written across the top, just above a note that attributed the job to a group of Turkish hackers. The site remained out of operation on Monday morning, June 19. The defacement led to rumors that the hackers may have used a new undisclosed vulnerability in the company's Internet Information Services 6.0 Web server. Microsoft dismissed these rumors on Monday, saying that the hack was due to a misconfigured Web server.
Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=cybercrime_hacking&articleId=900127 9&taxonomyId=82

38. *June 19, Security Focus* — **Cisco CallManager cross−site scripting vulnerability.** Cisco CallManager is prone to a cross−site scripting vulnerability. This issue is due to a failure in the Web−interface to properly sanitize user−supplied input. An attacker may leverage this issue to have arbitrary script code execute in the browser of an unsuspecting administrative user in the context of the affected site. This may help the attacker launch other attacks.
For a complete list of vulnerable products: http://www.securityfocus.com/bid/18504/info
Solution: Cisco has released an advisory to address this issue. Fixes are reportedly forthcoming.
For more information: http://www.securityfocus.com/bid/18504/references
Source: http://www.securityfocus.com/bid/18504/discuss

39. *June 19, eWeek* — **Microsoft posts Excel zero−day flaw workarounds.** Microsoft's security response center is recommending that businesses consider blocking Excel spreadsheet attachments at the network perimeter to help thwart targeted attacks that exploit an unpatched software vulnerability. The software giant published a pre−patch advisory on Monday, June 19, with a list of workarounds that include blocking Excel file−types at the e−mail gateway. File extensions associated with the widely deployed Microsoft Excel program are: xls, xlt, xla, xlm, xlc, xlw, uxdc, csv, iqy, dqy, rqy, oqy, xll, xlb, slk, dif, xlk, xld, xlshtml, xlthtml and xlv. The company's guidance comes just a few days after public confirmation that a new, undocumented Excel flaw was being used in an attack against an unidentified business target. The attack resembles a similar exploit that targeted Microsoft Word users, prompting suspicion among security researchers that the attacks may be linked.
Microsoft pre−patch advisory: http://www.microsoft.com/technet/security/advisory/921365.mspx

Source: http://www.eweek.com/article2/0,1895,1978835,00.asp

40. *June 19, Websense Security Labs* — **Malicious Website/Malicious Code: Soccer fan Trojan horses.** Websense Security Labs has reports of a new e−mail that is spoofed as a story about a group of soccer fans that have been killed by teenagers. The e−mail includes the subject: "soccer fans killed by five teens" and includes an attachment called "soccer_fans.jpg.exe". If the attachment is run, a Trojan horse downloader connects to a Website. The filename downloaded is called "dianaimag.exe". When that file runs, it attempts to disable Microsoft's Firewall and then visit another Website to download code.
Source: http://www.websense.com/securitylabs/alerts/alert.php?AlertI D=527

41. *June 16, Sophos* — **Spammed Trojan claims Bush/Blair Middle East oil cover−up.** Sophos has warned of a Trojan horse that has been spammed out to e−mail addresses disguised as a message claiming that George W. Bush and Tony Blair are conspiring with oil companies to push up petrol prices. Other disguises being used by the hackers to distribute the Trojan horse include news reports that Osama Bin Laden has been killed or Michael Jackson has committed suicide, CCTV photos of an alleged university rapist, and requests for a photograph to be approved for a magazine. The Troj/Stinx−W Trojan horse has been spammed out in e−mail messages, which can have a variety of subject lines including "Petrol Price Conspiracy," "Campus Student Raped," or "Bush and Blair Conspire."
Source: http://www.sophos.com/pressoffice/news/articles/2006/06/stin xw.html

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of active exploitation of a new vulnerability in Microsoft Excel. Successful exploitation could allow an attacker to execute arbitrary code with the privileges of the user running Excel. For more information please the review the following:

Technical Cyber Security Alert: TA06−167A
http://www.us−cert.gov/cas/techalerts/TA06−167A.html

Vulnerability Note: VU#802324 http://www.kb.cert.org/vuls/id/802324

We are continuing to investigate this vulnerability. US−CERT recommends the following actions to help mitigate the security risks:

Install anti−virus software, and keep its virus signature files up to date.

Limit user privileges to no administrator rights.

Save and scan any attachments before opening them.

Review the workarounds described in Microsoft Security Advisory 921365: http://www.microsoft.com/technet/security/advisory/921365.ms px

US−CERT strongly encourages users not to open unfamiliar or unexpected email attachments, even if sent by a known and trusted source. Users may wish to read Cyber Security Tip ST04−010 for more information on working with email attachments: http://www.us−cert.gov/cas/tips/ST04−010.html

FDIC Phishing Scam

US−CERT continues to receive reports of phishing scams that target online users. Recently, the phishing scam targeted the customers of Federal Deposit Insurance Company (FDIC) insured institutions.

Customers of FDIC institutions received a spoofed email message, which claims that their account is in violation of the Patriot Act, and that FDIC insurance has been removed from their account until their identity can be verified. The message provides a link to a malicious web site which prompts users to enter their customer account and identification information.

If you were affected by the FDIC phishing scam, please refer to the FDIC Consumer Alert for assistance: http://www.fdic.gov/consumers/consumer/alerts/phishing.html

US−CERT confirms that the federal agencies including Department of Homeland Security (DHS) mentioned in the fraudulent email have not sent out an email that requests customer account or identification information.

US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT: http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to OnGuard Online, a consortium of Federal Agencies: http://onguardonline.gov/phishing.html

Additionally, users are encouraged to take the following measures to prevent phishing attacks from occurring:

Do not follow unsolicited web links received in email messages.

Contact your financial institution and file a complaint with the Federal Trade Commission (FTC) immediately if you believe your account or financial information has been compromised.

https://rn.ftc.gov/pls/dod/widtpubl$.startup?Z_ORG_CODE=PU03

Review FTC's web site on how to protect yourself from identity theft: http://www.consumer.gov/idtheft/

Review the OnGuard Online practical tips to guard against Internet fraud, secure your computer, and protect your personal information: http://onguardonline.gov/phishing.html

Refer to the US−CERT Cyber Security Tip on Avoiding Social Engineering and Phishing Attacks: http://www.us−cert.gov/cas/tips/ST04−014.html

Refer to the CERT Coordination Center document on understanding Spoofed/Forged Email: http://www.cert.org/tech_tips/email_spoofing.html

PHISHING SCAMS

US−CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT. http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. http://onguardonline.gov/phishing.html

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 38566 (−−−), 445 (microsoft−ds), 25 (smtp), 24232 (−−−), 80 (www), 32790 (−−−), 113 (auth), 135 (epmap), 4672 (eMule) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer